

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-74882

(43) 公開日 平成11年(1999) 3月16日

(51) Int.Cl.⁸
H 0 4 L 12/14
G 0 6 F 13/00

識別記号
3 5 1

F I
H 0 4 L 11/02 F
G 0 6 F 13/00 3 5 1 A

審査請求 未請求 請求項の数 2 F D (全 12 頁)

(21) 出願番号 特願平9-249507

(22) 出願日 平成 9 年(1997) 8 月29日

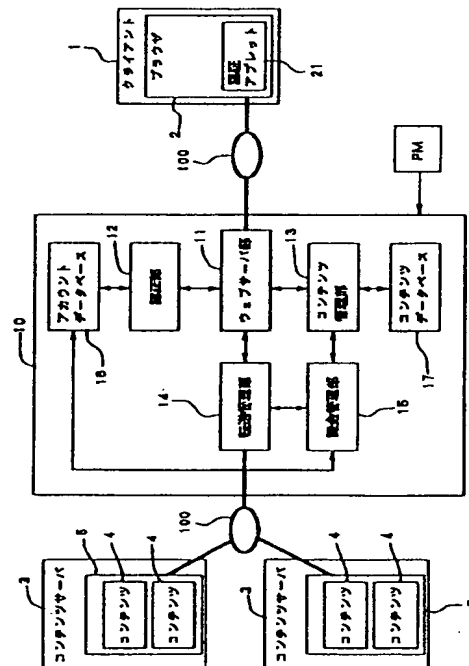
(71) 出願人 597131875
有限会社ネットベース
東京都千代田区内神田 1 丁目 2 番 1 号 M
TKビル7 階
(72) 発明者 西井 淳
東京都千代田区神田神保町三丁目11番地
望月ビル6 階 有限会社ネットベース内
(72) 発明者 柴本 浩之
東京都千代田区神田神保町三丁目11番地
望月ビル6 階 有限会社ネットベース内
(74) 代理人 弁理士 中村 猛

(54) 【発明の名称】 情報資源転送制御プログラムを記録したプログラム記録媒体

(57) 【要約】

【課題】 コンテンツの転送を一元的に管理し、適切な課金を行うこと。

【解決手段】 制御装置 10 は、コンテンツサーバ 3 のコンテンツ 4 に対するアクセスを一元的に管理しており、コンテンツ 4 は制御装置 10 を介してクライアント 1 に転送される。ユーザーが制御装置 10 にアクセスすると、認証部 12 により認証が行われる。正当なユーザーがコンテンツ 4 の URL を入力すると、コンテンツ 4 の課金タイプが設定される。コンテンツ 4 は、転送管理部 14 を介してクライアント 1 に転送される。コンテンツ 4 の利用状態は、課金管理部 15 により計測され、利用状態に応じた課金が行われる。



【特許請求の範囲】

【請求項1】 分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源の転送制御を行うための制御プログラムを記録したプログラム記録媒体において、情報資源の転送要求が正当であるか否かを判定する判定手段と、前記判定手段により正当な転送要求であると判定された場合には、前記転送要求された情報資源を当該転送要求発行元に対して転送する転送制御手段と、少なくとも前記情報資源の利用時間を含む利用状態を計測する計測手段とを、コンピュータに実現させるための制御プログラムをコンピュータが読取り及び理解可能な形態で記録してなるプログラム記録媒体。

【請求項2】 更に、前記転送要求発行元との間の接続が継続しているか否かを確認するための接続確認手段を前記コンピュータに実現させることを特徴とする請求項1に記載のプログラム記録媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、例えば、インターネットやイントラネット等の所定の通信プロトコルに従って複数のコンピュータ間で情報資源を転送する分散型情報閲覧環境下で用いられる情報資源転送制御プログラムを記録したプログラム記録媒体に関するものである。

【0002】

【従来の技術】 例えば、インターネットやイントラネット等として広く知られた分散型情報閲覧環境は、TCP/IP (Transmission Control Protocol/Internet Protocol)、HTTP (HyperText Transfer Protocol) 等の機種に依存しない所定のプロトコルに従ってデータ転送を行う複数のコンピュータを通信回線で相互接続することにより構成されている。この分散型情報閲覧環境下では、例えば、クライアント(情報資源の転送を要求するコンピュータ)からの転送要求に従って、サーバ(情報資源を提供するコンピュータ)は予め蓄積された情報資源をクライアントに転送するようになっている。

【0003】 例えば、HTML (HyperText Markup Language) と呼ばれる所定の言語で記述された情報資源 (HTMLドキュメント) は相互にリンク可能であり、各情報資源はURL (Uniform Resource Locator) と呼ばれる資源識別情報によって特定することができる。近年では、パーソナルコンピュータの性能向上と著しい普及、通信回線の整備等に支えられて、インターネット上の情報資源を利用するユーザーが増大している。ここで、インターネットへの接続方法を通信回線の種類に着目して分類すると、専用線接続とダイヤルアップ接続とに大別できる。専用線の導入にはコストがかかるため、通常のユーザーは、公衆電話回線を介してプロバイダと呼ばれる接続業者のネットワークに接続し、プロバイダのネットワーク端末としてインターネットに接続することが多い。

このような接続形態をダイヤルアップIP接続と呼ぶ。

【0004】 ダイヤルアップ接続すると、接続の度にユーザーのコンピュータにIPアドレスと呼ばれる識別情報が割り当てられる。そして、ユーザーが、例えば、いわゆるホームページ等の各種コンテンツの利用を希望すると、コンテンツを提供するサーバは、ユーザーのコンピュータに割り当てられたIPアドレスに向けて要求されたデータを転送する。これにより、ユーザーは、各サーバに蓄積された静止画像、動画、音楽等の種々のコンテンツを自由に楽しむことができる。

【0005】

【発明が解決しようとする課題】 ところで、近年では、いわゆるインターネット人口の爆発的增加に伴って、インターネットの商業的利用の活性化が望まれている。即ち、例えば、ビデオや通信カラオケ、ネットワーク対戦ゲーム等の価値あるコンテンツを適正な料金で提供することにより、コンテンツ制作費用を回収すると共に、より優れたコンテンツを提供可能とする新たなシステムが望まれている。

【0006】 このようなインターネットの商業的利用は、コンテンツの利用状態を正しく計測できる課金システムによって支えられる。しかし、従来のインターネットは、情報の共有及び公開を主要な目的とするため、コンテンツの利用状態を正確に把握することができない。

一例を挙げれば、ユーザーがWWW (World-Wide Web) ブラウザによってウェブサーバ上のコンテンツを利用する場合、通常、ウェブサーバ側では、アクセスされた事実と、このアクセス元のIPアドレス等の僅かな情報のみしか検出できない。従って、誰かが何かを利用していることは検出できても、どこの誰がどのコンテンツを利用しているかは不明であるため、利用料金を請求すべき者を特定することができない。特に、ダイヤルアップIP接続の場合には、接続の度にIPアドレスが変更されるため、IPアドレスのみで利用者を特定することはできない。

【0007】 もっとも、HTTPは、単純なアクセス認証の機能を有するから、このアクセス認証機能を利用すれば、特定の者にのみコンテンツの利用を許可することも可能である。しかし、かかるアクセス認証はウェブページ毎に設定可能であるため、ウェブページ毎にアクセス認証を行う必要がある。これに加えて、ウェブサーバは、ウェブページを1枚送信した時点で通信を終了するため、同一ユーザーが同一のIPアドレスで再度アクセスした場合でも、再びアクセス認証を行う必要がある。従って、従来システムでは、認証作業が不便であり、各サーバ上の各種コンテンツをスムーズに利用することができないという問題がある。

【0008】 また、従来技術では、ユーザーによるコンテンツ利用が終了したことを知ることはできないため、利用時間やデータ転送量を検出することができず、利用

時間やデータ転送量に応じて料金を請求する従量制の課金を行うことができないという問題がある。

【0009】さらに、近年では、インターネット上に仮想オフィス、仮想企業等を設立し、これらの仮想オフィス等に各メンバーがアクセスしてデータやプログラムを交換することにより、地域的に分散した複数のメンバーによってジョブを遂行するシステムも普及し始めている。かかる仮想オフィスシステムの場合にも、構成メンバーの認証と各メンバーによるコンテンツの利用状態の把握が必要とされるが、課金システムと同様に、従来のインターネット技術では、このような認証及び利用状態の把握を実現するのが困難であった。

【0010】本発明は、上記のような種々の課題に鑑みなされたものであり、その目的は、分散型情報閲覧環境下において、情報資源の転送制御を行うことにより認証及び利用状態を管理できるようにするための情報資源転送制御プログラムを記録したプログラム記録媒体を提供することにある。

【0011】

【課題を解決するための手段】本発明に係るプログラム記録媒体は、分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源の転送制御を行うための制御プログラムを記録したプログラム記録媒体において、情報資源の転送要求が正当であるか否かを判定する判定手段と、前記判定手段により正当な転送要求であると判定された場合には、前記転送要求された情報資源を当該転送要求発行元に対して転送する転送制御手段と、少なくとも前記情報資源の利用時間を含む利用状態を計測する計測手段とを、コンピュータに実現させるための制御プログラムをコンピュータが読取り及び理解可能な形態で記録したことを特徴とする。

【0012】ここで、「分散型情報閲覧環境」とは、複数のコンピュータに分散された各種情報資源を利用可能な環境を意味し、具体的には、例えば、いわゆるインターネットやイントラネット等の所定プロトコルに従って情報資源を転送するネットワーク環境が含まれる。「情報資源」とは、利用される各種データやプログラム等を意味し、具体的には、例えば、動画像データ、静止画像データ、テキストデータ、HTMLドキュメント、データベース、楽曲データ、音声データ、ゲームプログラム、ドキュメント作成プログラム、画像生成プログラム等が含まれる。「プログラム記録媒体」には、例えば、フロッピーディスク（FD）、コンパクトディスク（CD）、ハードディスク（HD）、デジタルビデオディスク（DVD）、メモリーカード、磁気テープ等のプログラムを記録できる各種媒体を含むほか、例えば、通信回線を介してリモートダウンロードする等のように、通信媒体を介してプログラムを転送記録する場合も含む。「転送要求が正当であるか否か」とは、正当な利用権限を有するクライアントからの転送要求であるか否かの意味であ

り、具体的には、例えば、識別番号（ID）やパスワード等の各種認証情報に基づいて判定することができる。また、「転送要求発行元」とは、転送要求を発行したクライアントの意味である。「利用時間」とは、情報資源を利用した時間であり、例えば、利用開始時刻と利用終了時刻との差分によって検出することができる。「利用状態」とは、情報資源を利用している状態の意味であり、具体的には、データ転送量、利用時間等が含まれる。

【0013】例えば、ネットワーク対戦ゲームやウェブページ等の利用を希望するユーザーは、URL等の資源識別情報によって所望の情報資源を特定し、該情報資源の転送を要求する。判定手段は、この転送要求が正当であるか否かを判定する。正当な転送要求ではない場合は、該転送要求を拒否すればよい。正当な転送要求の場合には、転送制御手段によって情報資源が転送され、ユーザーは転送された情報資源を利用する。計測手段は、少なくとも情報資源の利用時間を含む利用状態を計測する。従って、利用時間、データ転送量、転送されたウェブページ数等の利用状態を把握することができ、利用状態に応じて課金することが可能となる。

【0014】更に、前記転送要求発行元ととの間の接続が継続しているか否かを確認するための接続確認手段を前記コンピュータに実現させることもできる。

【0015】接続確認手段によって転送要求発行元ととの間の接続が継続していることを確認することにより、少なくとも情報資源の利用時間を容易に把握できる。

【0016】

【発明の実施の形態】以下、図1～図9に基づき本発明の実施の形態について詳述する。

【0017】図1には、情報資源転送制御システムの機能構成の要部が示されている。本システムは、例えば、フロッピーディスクやコンパクトディスク等のプログラム記録媒体PMに記録された所定のプログラムをコンピュータに読み込ませることにより、実現することもできる。

【0018】通信回線100を介してインターネットに接続されたクライアント1には、ブラウザ2が実装されている。一方、通信回線100を介してインターネットに接続されたコンテンツサーバ3には、各種プログラムやデータ等の「情報資源」としてのコンテンツ4が記憶されている。各コンテンツ4は、コンテンツサーバ3が備えるウェブサーバ機能（図示せず）により転送される。ここで、各コンテンツサーバ3では、アクセス制限領域5を設けることにより、各コンテンツ4に対する無制限な利用を禁止している。このアクセス制限領域5は、予め指定されたIPアドレス以外からの転送要求を排除するためのものであり、具体的には、例えば、htaccess等のアクセス制御プログラムによって実現することができる。なお、htaccessとは、UNIX版サーバで利用可

能なアクセス制御のための定義ファイルであり、httpd (hypertext transfer protocol daemon) が参照するディレクトリの配下に置かれていれば、該ディレクトリ下に関してアクセス制御を適用できるものである。但し、これに限らず、サーバのOS環境等に応じて、種々のアクセス制限プログラムを利用できる。

【0019】クライアント1と各コンテンツサーバ3との間には、本発明に特徴的な情報資源転送制御装置10 (以下、制御装置10と略記) が設けられている。制御装置10は、クライアント1と各コンテンツサーバ3との間でhttpリクエスト及びレスポンスを中継等するものであり、いわゆるプロキシサーバまたはゲートウェイの一種である。従って、制御装置10は、アクセス制限領域5によるアクセス制限を受けず、各コンテンツサーバ3との間でデータ転送等を行うことができるようになっている。換言すれば、各コンテンツサーバ3には、制御装置10を介してのみアクセスすることができる。従って、コンテンツサーバ3側には、未登録のIPアドレスからアクセスするユーザーに対して、制御装置10のURLを紹介する機能を設けるのが好ましい。

【0020】制御装置10は、コンテンツ4の表示等を行うためのウェブサーバ部11と、制御装置10にアクセスしたユーザーの認証を行うための認証部12と、各コンテンツ4のコンテンツ情報を管理するコンテンツ管理部13と、コンテンツサーバ3からクライアント1に向けて流れる情報の転送を制御する転送管理部14と、情報の転送状態、即ち、コンテンツの利用状態に基づいて課金処理を行う課金管理部15とを含んで構成されている。また、制御装置10には、登録されたユーザーの認証情報等を記憶管理するアカウントデータベース16と、コンテンツ情報を記憶管理するコンテンツデータベース17とが設けられている。後述のように、制御装置10は、認証された正当なユーザーからの転送要求に応じて、所定のコンテンツサーバ3からコンテンツ4を入手し、該コンテンツ4をクライアント1に転送すると共に、コンテンツ利用状態に応じた課金処理を実行するようになっている。また、転送管理部14は、例えば、所定サイズ単位、所定時間単位でデータ転送を制御することができるようになっている。

【0021】図2には、アカウントデータベース16の一例が示されている。アカウントデータベース16には、例えば、ユーザー名、識別番号(ID)、パスワード、アカウントタイプ、金額、年齢等を記憶することができる。ここで、識別番号及びパスワードは、正当なユーザーであるか否かを判定するために用いられる認証情報である。アカウントタイプとは、支払い方法による種別を示す情報であり、例えば、予めクレジットカード番号等を登録したユーザーであれば、利用料金を加算して支払う加算型として記憶され、一方、クレジットユーザー以外のユーザーである場合は、予め購入した利用ボイ

ント等から利用した分を減算する減算型のユーザーとして記憶される。年齢情報は、例えば、コンテンツ4の利用に際して年齢制限が設定されている場合に参照されるものである。金額とは、利用金額の意味であり、加算型課金の場合は加算金額が記憶され、減算型課金の場合は残金額が記憶される。なお、図2に示す情報に限らず、例えば、職業、性別、住所、所属部署、利用回数等の他の情報も記憶させることができる。

【0022】図3には、コンテンツデータベース17の一例が示されている。コンテンツデータベース17には、コンテンツ名、課金タイプ、URL、課金単位、課金額、アクセス制限の条件等を記憶することができる。ここで、課金タイプとは、例えば、利用したウェブページの枚数に応じて課金される「ページ課金」、利用時間に応じて料金を請求する「時間従量」、データ転送量に応じて請求する「転送サイズ」等の種々の課金タイプを示す情報である。なお、複数の課金タイプを組み合わせることも可能である。URLとは、コンテンツ4の所在を特定するための資源識別情報である。課金単位とは、課金される利用単位を示し、例えば、所定時間、所定データサイズ等を用いることができる。課金額とは、課金単位毎に設定された料金である。但し、課金額の単位は、通貨単位(例えば我国の円)に限らず、例えば、ポイント等の他の単位を用いることができる。制限事項とは、例えば、未成年者不可、女性専用、技術部専用等のように、コンテンツの利用に際して課せられた条件を示す情報である。なお、図3に示す情報に限らず、例えば、ファイルサイズ、ファイルフォーマット形式、タイムスタンプ、コンテンツ提供者名等の他の情報も記憶させることができる。

【0023】図1に戻る。クライアント1が制御装置10にアクセスすると、制御装置10からクライアント1に認証アプレット21が転送され、認証アプレット21はクライアント1で起動する。この認証アプレット21は、例えば、米国サンマイクロシステムズ社が開発したJava言語等のアーキテクチャ・ニューラル言語で記述されたプログラムであり、制御装置10との間でデータ通信を行うようになっている。なお、認証アプレット21は、必ずしも制御装置10側から転送させる必要はない。例えば、クライアント1側に認証プログラムを予めインストールしておけば、該認証プログラムを起動させることにより、認証を行うこともできるからである。また、同様に、認証プログラムの全体をクライアント1側に転送する必要もない。クライアント1側に用意されている各種実行ファイルを適宜呼び出すことにより、認証プログラムを構成することもできるからである。

【0024】認証アプレット21が起動すると、クライアント1側のディスプレイ装置には、図4に示すような画面が表示される。この画面を認証画面と呼ぶ。認証画面には、ユーザーの識別番号を入力するためのID入力

部21Aと、パスワード入力部21Bと、制御装置10との接続を指示する接続指示部21Cと、制御装置10側から転送された各種メッセージ等を表示するための表示部21Dとを備えている。ID入力部21Aに入力されたIDとパスワード入力部21Bに入力されたパスワードとは、制御装置10に送信され、認証部12による判定を受ける。また、制御装置10からの接続確認の問い合わせを受信すると、認証アプレット21は、接続継続中の応答を返すようになっている。つまり、認証アプレット21は、認証情報入力手段と「接続確認手段」の少なくとも一部を構成するものとして把握することもできる。

【0025】図5は、クライアント1、制御装置10、コンテンツサーバ3の間の通信状態の概略を示す説明図である。

【0026】まず、クライアント1が制御装置10にアクセスすると、制御装置10は、クライアント1に認証アプレット21を転送する。認証アプレット21がクライアント1側で起動すると、ユーザーは、ID及びパスワードを入力する。これらのID及びパスワードは、制御装置10に送信され、正当なユーザーか否かの認証が行われる。予め登録された正当なユーザーである場合は、制御装置10からクライアント1に認証確認通知が送信される。

【0027】これによりアクセスが許可されたユーザーは、所望のコンテンツ4のURLを送信する。制御装置10は、指示されたコンテンツ4を転送する前に、認証アプレット21に対して接続確認の要求を行う。認証アプレット21が接続確認要求に応答することにより、要求されたコンテンツ4をクライアント1に転送することができる。認証アプレット21が終了している場合、または、クライアント1との通信パスが成立していない場合には、制御装置10はクライアント1からの接続確認信号を受信することができない。例えば、所定時間内に接続確認信号を受信できない場合は、コンテンツ4の転送は行われない。

【0028】認証アプレット21から接続確認の応答があった場合は、制御装置10は、所定のコンテンツサーバ3にアクセスして指定されたコンテンツ4を取り出し、このコンテンツ4をクライアント1に転送する。また、制御装置10は、利用時間やデータ転送量等の利用状態を計測し、利用状態に応じた課金を行う。

【0029】次に、図6～図9に基づいて本実施の形態の作用を説明する。なお、以下の説明では、ステップを「S」と略記する。まず、図6には、情報資源転送制御システムが行う処理の全体の流れが示されている。本システムの処理は、ユーザー認証を行う認証処理(S1)と、コンテンツ4を転送し課金する課金転送処理(S2)と、課金終了処理(S3)とに大別することが可能である。

【0030】図7には、認証処理のフローチャートが示されている。ユーザーが通信回線100を介して制御装置10にアクセスすると(S11)、制御装置10は、認証アプレット21をクライアント1に転送する(S12)。認証アプレット21が起動すると(S13)、ユーザーは、認証アプレット21にID及びパスワードを入力する(S14)。これらのID及びパスワードは、制御装置10の認証部12に入力され、これにより、認証部12は、アカウントデータベース16を参照する(S15)。

【0031】認証部12は、ID及びパスワードに基づいて、登録された正当なユーザーであるか否か、つまり、正当なアクセス権限を有するクライアント1からの転送要求であるか否かを判定する。例えば、IDを検索キーとしてアカウントデータベース16を検索した結果、入力されたパスワードと予め登録されたパスワードとが一致する場合には、正当なユーザーであると判定できる。これに対し、入力されたIDがアカウントデータベース16に登録されていない場合や、入力されたパスワードと登録されたパスワードとが一致しない場合には、正当なユーザーであると判定しない。

【0032】正当なユーザーであると判定された場合には、認証アプレット21に対し認証確認が通知される(S17)。この認証確認通知により、ユーザーにアクセスが許可される。一方、正当なユーザーではないと判定された場合、エラー処理が行われる(S18)。エラー処理としては、例えば、パスワード不一致、ID未登録等の表示を行い、再度の入力を促すことができる。

【0033】次に、図8は、課金転送処理を示すフローチャートである。図7と共に述べた認証処理によってアクセス許可を得たユーザーは、所望のコンテンツを示すURLをブラウザ2に入力する(S21)。このユーザーからのURLがコンテンツ管理部13に入力されると、コンテンツ管理部13は、コンテンツデータベース17を参照する(S22)。

【0034】コンテンツ管理部13は、要求されたコンテンツ4に制限事項が設定されているか否かを検出し、制限事項が設定されている場合には、この制限をクリアしているか否かを判定する(S23)。設定された制限をクリアしていないユーザーの場合は、例えば、設定されている制限事項と該制限事項を満足しない旨とを表示する等のように、エラー処理を行う(S24)。

【0035】所定の制限をクリアした場合には、要求されたコンテンツ4が有料であるか否かを判定する(S25)。例えば、コンテンツデータベース17の課金額に0がセットされているコンテンツ4は無料であると判定することができる。無料のコンテンツ4の場合は、所定のコンテンツサーバ3から要求されたコンテンツ4を取り出し、該コンテンツ4をクライアント1に転送する(S26)。なお、本システムを仮想商店街等の商業的

利用に用いる場合、コンテンツ4が無料ならば、データ転送量や利用時間等の利用状態を計測する必要はない。但し、仮想商店街の消費者動向等を調査する場合や仮想オフィス等で用いる場合等には、無料のコンテンツであっても利用状態を計測する利益がある。

【0036】要求されたコンテンツ4が有料の場合は、該コンテンツ4の課金タイプが読み出され、この課金タイプは課金管理部15に設定される(S27)。課金管理部15は、アカウントデータベース16を参照し(S28)、次に、アカウントタイプが減算型であるか否かを判定する(S29)。減算型課金ではない場合、即ち、利用した分だけ料金が加算される加算型課金の場合には、認証アプレット21に対して接続確認を行い(S30)、クライアント1と制御装置10との間の接続を確認してから、要求されたコンテンツ4をクライアント1に転送する(S31)。また、コンテンツ4の利用状態、例えば、利用時間やデータ転送量が計測され、この利用状態に基づいて課金される(S31)。課金結果は、アカウントデータベース16に書き戻される。また、課金結果をクライアント1側に通知してもよい。

【0037】一方、例えば、予め購入したポイントから利用した分のポイントを減算する減算型課金の場合は、利用可能残高としてのポイント残があるか否かを判定する(S32)。ポイント残が無い場合は、ポイント残がない旨を通知する等のエラー処理が行われる(S33)。エラー処理を行う場合、要求されたコンテンツ4はクライアント1に転送されない。

【0038】ポイント残がある場合には、S30と同様に認証アプレット1との間で接続確認を行い(S34)、要求されたコンテンツ4を所定のコンテンツサーバ3から取り出してクライアント1に転送する(S35)。また、例えば、利用時間やデータ転送量等の利用分に応じてポイントを減算することにより、課金が行われる(S35)。

【0039】次に、図9には、課金転送の終了を監視する課金終了処理が示されている。課金転送の終了は、幾つかの終了条件のうちいずれか一つの条件が成立することにより行われる。

【0040】即ち、例えば、認証アプレット21との間で接続確認をできなかった場合(S41)、ユーザーが終了を示す特定のURLを入力した場合(S42)、アカウントデータベース16に記憶されたポイント残がなくなった場合(S43)、要求されたコンテンツ4を全て転送した場合(S44)に、課金処理は終了される(S45)。なお、S42で述べた特定の終了URLを入力した場合について説明する。例えば、ウェブページに課金開始URL(スタートボタン等)と課金終了URL(ストップボタン等)とを設けておき、課金開始URLを入力すると課金を開始し、課金終了URLを入力すると課金を終了させる構成の場合に用いられるものであ

る。認証アプレット21自体の起動が終了された場合、クライアント1と制御装置10との間の通信バスが切断された場合には、接続終了と判断されて(S41)課金処理が終了する(S45)。

【0041】このように構成される本実施の形態によれば、以下の効果を奏する。

【0042】第1に、制御装置10は、コンテンツサーバ3とクライアント1との間に介在して、クライアント1からの転送要求とコンテンツサーバ3からのコンテンツ取り出しとを一元的に管理するため、コンテンツ4の利用状態を正確に計測することができ、利用状態に基づいた課金を行うことができる。

【0043】第2に、全てのコンテンツ4は、制御装置10の転送管理部14によって転送が管理されているため、例えば、1KBずつ等のような転送サイズ単位や1分間毎のような所定時間単位で、コンテンツ4を所定単位に分けて少しずつ転送することができる。従って、コンテンツ4の性質等に応じてきめ細かく転送を行うことができるため、購入ポイント残や利用時間等のような利用状態に応じた課金を行うことができる。

【0044】第3に、クライアント1の認証は制御装置10の認証部12で一元的に行われ、また、コンテンツサーバ3から取り出されたコンテンツ4は全て制御装置10のウェブサーバ部11を介して表示されるため、ユーザーは、通常のブラウジングと同一の操作環境で各種の有料コンテンツを滑らかに利用することができ、使い勝手が向上する。つまり、従来のインターネット技術ではウェブページ単位での認証は可能であるが、ウェブページ毎にID及びパスワードを入力するのでは大変手間がかかり、コンテンツ利用意欲も低下する。これに対し、本発明では、コンテンツ4の利用を一元的に管理する制御装置10との間で1回認証を行えばよく、認証後は所望のURLを入力するだけで必要なコンテンツ4を利用することができ、何らの違和感なく各種コンテンツ4を利用することができる。

【0045】第4に、クライアント1側で起動する認証アプレット21との間で接続確認を行うため、接続の度にIPアドレスが変化するダイヤルアップIP接続の場合でも、特定の正当なユーザーとの接続状態が継続していることを確実に検出することができる。従って、ユーザーの利用状態を把握することができ、正確な課金を行うことができる。

【0046】第5に、各コンテンツ4毎に利用状態を把握することができるため、各コンテンツ4のオーナーがそれぞれ異なる場合でも、課金収入を正しく分配することができる。つまり、一つのコンテンツサーバ3によって提供可能なコンテンツ4は、それぞれ別のオーナーによって所有されている場合がある。この場合、従来のインターネット技術では、コンテンツ4毎の利用状態を把握できないため、コンテンツサーバ3単位で徴収した課金を

利用に用いる場合、コンテンツ4が無料ならば、データ転送量や利用時間等の利用状態を計測する必要はない。但し、仮想商店街の消費者動向等を調査する場合や仮想オフィス等で用いる場合等には、無料のコンテンツであっても利用状態を計測する利益がある。

【0036】要求されたコンテンツ4が有料の場合は、該コンテンツ4の課金タイプが読み出され、この課金タイプは課金管理部15に設定される(S27)。課金管理部15は、アカウントデータベース16を参照し(S28)、次に、アカウントタイプが減算型であるか否かを判定する(S29)。減算型課金ではない場合、即ち、利用した分だけ料金が加算される加算型課金の場合には、認証アプレット21に対して接続確認を行い(S30)、クライアント1と制御装置10との間の接続を確認してから、要求されたコンテンツ4をクライアント1に転送する(S31)。また、コンテンツ4の利用状態、例えば、利用時間やデータ転送量が計測され、この利用状態に基づいて課金される(S31)。課金結果は、アカウントデータベース16に書き戻される。また、課金結果をクライアント1側に通知してもよい。

【0037】一方、例えば、予め購入したポイントから利用した分のポイントを減算する減算型課金の場合は、利用可能残高としてのポイント残があるか否かを判定する(S32)。ポイント残が無い場合は、ポイント残がない旨を通知する等のエラー処理が行われる(S33)。エラー処理を行う場合、要求されたコンテンツ4はクライアント1に転送されない。

【0038】ポイント残がある場合には、S30と同様に認証アプレット1との間で接続確認を行い(S34)、要求されたコンテンツ4を所定のコンテンツサーバ3から取り出してクライアント1に転送する(S35)。また、例えば、利用時間やデータ転送量等の利用分に応じてポイントを減算することにより、課金が行われる(S35)。

【0039】次に、図9には、課金転送の終了を監視する課金終了処理が示されている。課金転送の終了は、幾つかの終了条件のうちいずれか一つの条件が成立することにより行われる。

【0040】即ち、例えば、認証アプレット21との間で接続確認をできなかった場合(S41)、ユーザーが終了を示す特定のURLを入力した場合(S42)、アカウントデータベース16に記憶されたポイント残がなくなった場合(S43)、要求されたコンテンツ4を全て転送した場合(S44)に、課金処理は終了される(S45)。なお、S42で述べた特定の終了URLを入力した場合について説明する。例えば、ウェブページに課金開始URL(スタートボタン等)と課金終了URL(ストップボタン等)とを設けておき、課金開始URLを入力すると課金を開始し、課金終了URLを入力すると課金を終了させる構成の場合に用いられるものであ

る。認証アプレット21自体の起動が終了された場合、クライアント1と制御装置10との間の通信バスが切断された場合には、接続終了と判断されて(S41)課金処理が終了する(S45)。

【0041】このように構成される本実施の形態によれば、以下の効果を奏する。

【0042】第1に、制御装置10は、コンテンツサーバ3とクライアント1との間に介在して、クライアント1からの転送要求とコンテンツサーバ3からのコンテンツ取り出しとを一元的に管理するため、コンテンツ4の利用状態を正確に計測することができ、利用状態に基づいた課金を行うことができる。

【0043】第2に、全てのコンテンツ4は、制御装置10の転送管理部14によって転送が管理されているため、例えば、1KBずつ等のような転送サイズ単位や1分間毎のような所定時間単位で、コンテンツ4を所定単位に分けて少しずつ転送することができる。従って、コンテンツ4の性質等に依じてきめ細かく転送を行うことができるため、購入ポイント残や利用時間等のような利用状態に応じた課金を行うことができる。

【0044】第3に、クライアント1の認証は制御装置10の認証部12で一元的に行われ、また、コンテンツサーバ3から取り出されたコンテンツ4は全て制御装置10のウェブサーバ部11を介して表示されるため、ユーザーは、通常のブラウジングと同一の操作環境で各種の有料コンテンツを滑らかに利用することができ、使い勝手が向上する。つまり、従来のインターネット技術ではウェブページ単位での認証は可能であるが、ウェブページ毎にID及びパスワードを入力するのでは大変手間がかかり、コンテンツ利用意欲も低下する。これに対し、本発明では、コンテンツ4の利用を一元的に管理する制御装置10との間で1回認証を行えばよく、認証後は所望のURLを入力するだけで必要なコンテンツ4を利用することができ、何らの違和感なく各種コンテンツ4を利用することができる。

【0045】第4に、クライアント1側で起動する認証アプレット21との間で接続確認を行うため、接続の度にIPアドレスが変化するダイヤルアップIP接続の場合でも、特定の正当なユーザーとの接続状態が継続していることを確実に検出することができる。従って、ユーザーの利用状態を把握することができ、正確な課金を行うことができる。

【0046】第5に、各コンテンツ4毎に利用状態を把握することができるため、各コンテンツ4のオーナーがそれぞれ異なる場合でも、課金収入を正しく分配することができる。つまり、一つのコンテンツサーバ3によって提供可能なコンテンツ4は、それぞれ別のオーナーによって所有されている場合がある。この場合、従来のインターネット技術では、コンテンツ4毎の利用状態を把握できないため、コンテンツサーバ3単位で徴収した課金を

各コンテンツオーナーに正しく分配することができない。これに対し、本発明では、各コンテンツ4毎に利用状態を把握できるため、各コンテンツオーナーに対して公平に課金収入を分配することができる。

【0047】第6に、コンテンツ情報を記憶管理するコンテンツデータベース17を有するため、ユーザーのURL入力だけでコンテンツ4の課金タイプを容易に知ることができる。

【0048】なお、本発明は、上述した実施の形態に限らず、種々の変形等を行うことができる。例えば、制御装置10を単一のコンピュータ上に実現する必要はなく、複数のコンピュータを連携させて制御装置10の機能を実現してもよい。

【0049】また、クライアント1と制御装置10の間の接続確認は、認証アプレット21以外のブラウザやOS（オペレーティングシステム）との間で行うようにしてもよい。

【0050】さらに、コンテンツ4の一部または全部を制御装置4に蓄積する構成としてもよい。また、例えば、制御装置10から衛星通信回線や地上波放送等を利用してクライアント1に転送するようにしてもよい。

【0051】さらに、本発明は、有料コンテンツ4を集積した仮想商店街、仮想デパート等に好適に用いることができるほか、仮想オフィス等でのいわゆるインターネットワーキングにも適用することができる。

【0052】なお、上述した実施の形態は、例えば、以下のように種々のカテゴリで多段階に表現することもできる。

【0053】表現1. 分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源4の転送制御を行う情報資源転送制御システムにおいて、情報資源4の転送要求が発生すると、該転送要求が正当な転送要求であるか否かを判定し、正当な情報資源転送要求であると判定した場合には、前記転送要求に係る情報資源4を転送すると共に、前記情報資源4の利用状態を計測する制御手段10を設けたことを特徴とする情報資源転送制御システム。

【0054】表現2. 前記利用状態には、少なくとも利用時間が含まれている表現1に記載の情報資源転送制御システム。

【0055】表現3. 前記情報資源4は、所定単位ずつ転送可能である表現1に記載の情報資源転送制御システム。

【0056】表現4. 分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源4の転送制御を行う情報資源転送制御装置において、情報資源4の転送要求が正当であるか否かを判定する判定手段12と、前記判定手段12により正当な転送要求であると判定された場合には、前記転送要求された情報資源4を当該転送要求発行元1に対して転送する転送制御手段14と、少なくとも

前記情報資源4の利用時間を含む利用状態を計測する計測手段15とを設けたことを特徴とする情報資源転送制御装置。

【0057】表現5. ユーザーの認証情報を含むユーザー情報を管理するユーザー情報管理手段16と、情報資源4の課金タイプを含む資源情報管理手段17とを設け、前記判定手段12は前記ユーザー情報管理手段16を参照して正当な転送要求であるか否かを判定し、前記計測手段15は前記資源情報管理手段17を参照して前記利用状態を計測する表現4に記載の情報資源転送制御装置。

【0058】表現6. 前記転送要求発行元1との間で接続が継続していることを確認するための接続確認手段21を設け、該接続確認手段21の確認信号を参照して前記計測手段による利用状態の計測を行う表現4または表現5に記載の情報資源転送制御装置。

【0059】表現7. 分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源4の転送制御を行う情報資源転送制御方法において、情報資源4の転送要求が発生すると、該転送要求が正当な転送要求であるか否かを判定し（S11～S18）、正当な情報資源転送要求であると判定した場合には、前記転送要求に係る情報資源4を転送すると共に、前記情報資源4の利用状態を計測する（S21～S35）ことを特徴とする情報資源転送制御方法。

【0060】表現8. 分散型情報閲覧環境を構築する複数のコンピュータ間で情報資源4の転送制御を行う情報資源転送制御方法において、情報資源の転送要求が正当な転送要求であるか否かを判定するステップ（S1）と、正当な転送要求であると判定された場合には、情報資源4のアクセス制限条件を満たすか否かを判定するステップ（S23）と、アクセス制限条件を満たすと判定された場合には、前記情報資源の転送要求発行元1との間で接続が継続していることを確認するステップ（S30、S34）と、接続が確認された場合には前記転送要求に係る情報資源4を前記転送要求発行元1に転送するステップ（S31、S35）とを含んでなることを特徴とする情報資源転送制御方法。

【0061】

【発明の効果】以上説明した通り、本発明に係る情報資源転送制御プログラムを記録したプログラム記録媒体によれば、情報資源の転送を一元的に管理することができ、認証された特定のユーザーからの転送要求に応じて情報資源を転送することができ、情報資源の利用状態を計測することができる。

【図面の簡単な説明】

【図1】本発明に係る情報資源転送制御プログラムを記録したプログラム記録媒体をコンピュータに読み込ませることにより実現される情報資源転送制御システムの全体構成を示すブロック図である。

【図2】アカウントデータベースの構成を示す説明図である。

【図3】コンテンツデータベースの構成を示す説明図である。

【図4】認証アプレットによる認証画面を示す説明図である。

【図5】クライアント、制御装置及びコンテンツサーバ間の転送タイミング等の概略を示す説明図である。

【図6】コンテンツ転送制御処理の全体を示すフローチャートである。

【図7】認証処理を示すフローチャートである。

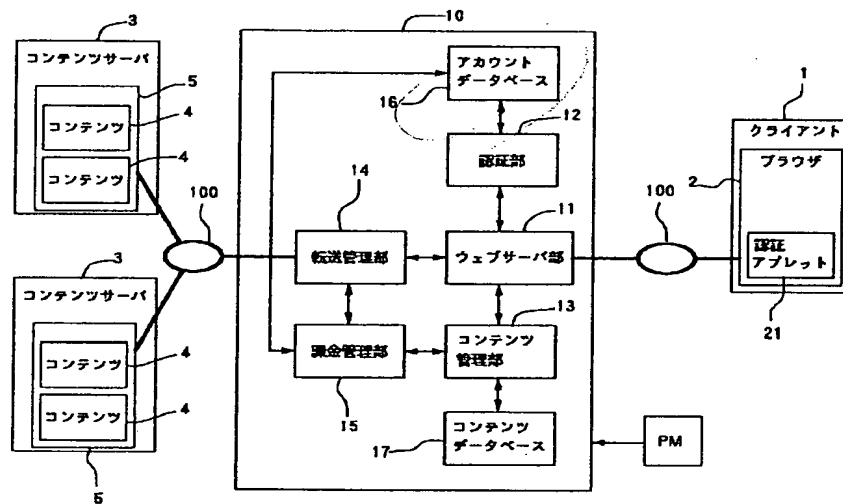
【図8】課金転送処理を示すフローチャートである。

【図9】課金終了処理を示すフローチャートである。

【符号の説明】

- 1 クライアント
- 3 コンテンツサーバ
- 4 コンテンツ
- 10 制御装置
- 11 ウェブサーバ部
- 12 認証部
- 13 コンテンツ管理部
- 14 転送管理部
- 15 課金管理部
- 16 アカウントデータベース
- 17 コンテンツデータベース
- 21 認証アプレット

【図1】



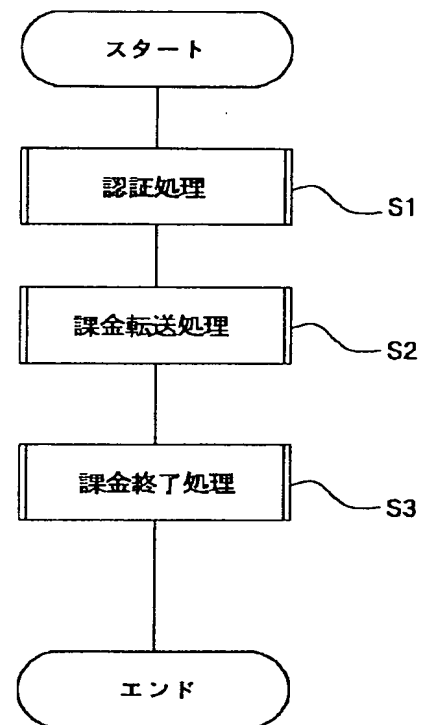
【図2】

ユーザ名	ID	パスワード	アカウント タイプ	金額	年齢
USER1	ID1	PASS1	加算型	2500	36
USER2	ID2	PASS2	減算型	100	19

【図3】

コンテンツ名	課金タイプ	URL	課金単位	課金額	制限事項
CONT1	ページ課金	URL1		2	なし
CONT2	時間従量	URL2	10秒	10	未成年不可
CONT3	転送サイズ	URL3	10Kbyte	5	なし

【図6】

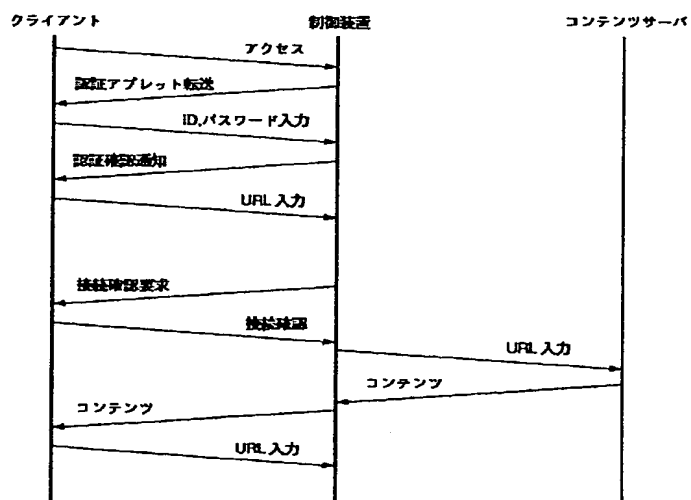


【図4】

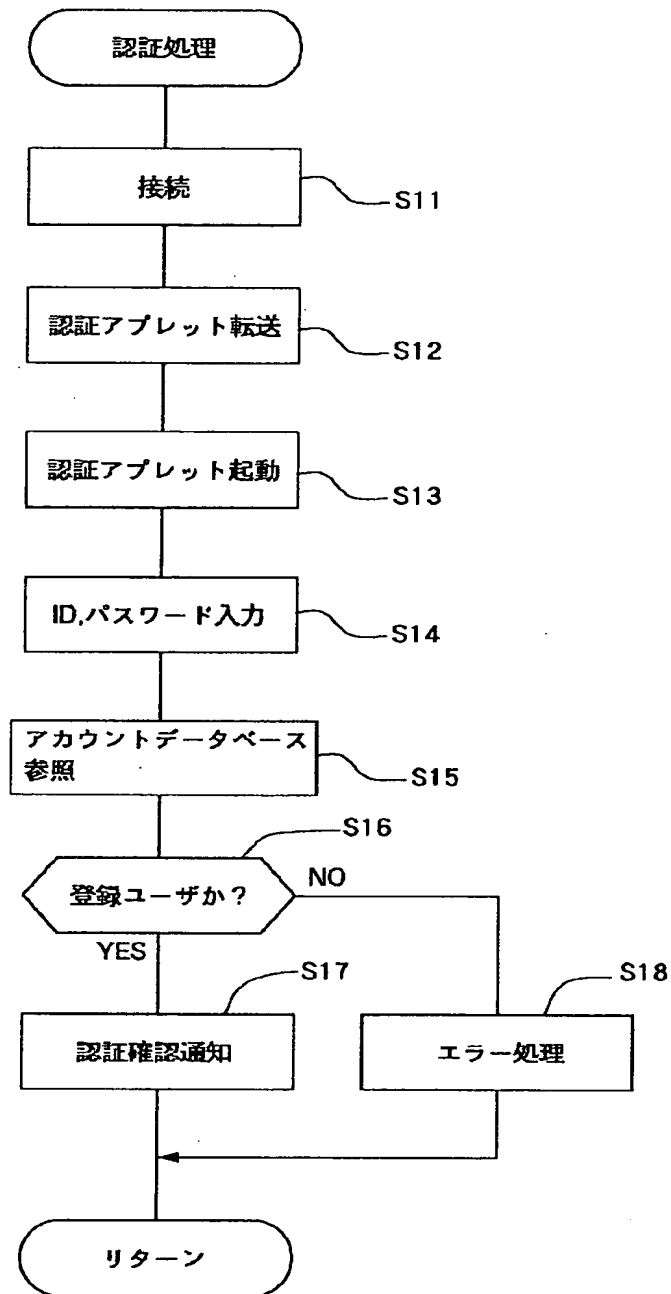
Figure 4 shows a screenshot of a web application interface (21). It contains the following elements:

- ID input field (21A) with the value 376600119.
- Password input field (21B) with masked characters (*****).
- Submit button (21C) labeled 接続 (Connect).
- Message display area (21D) labeled メッセージ表示 (Message Display).

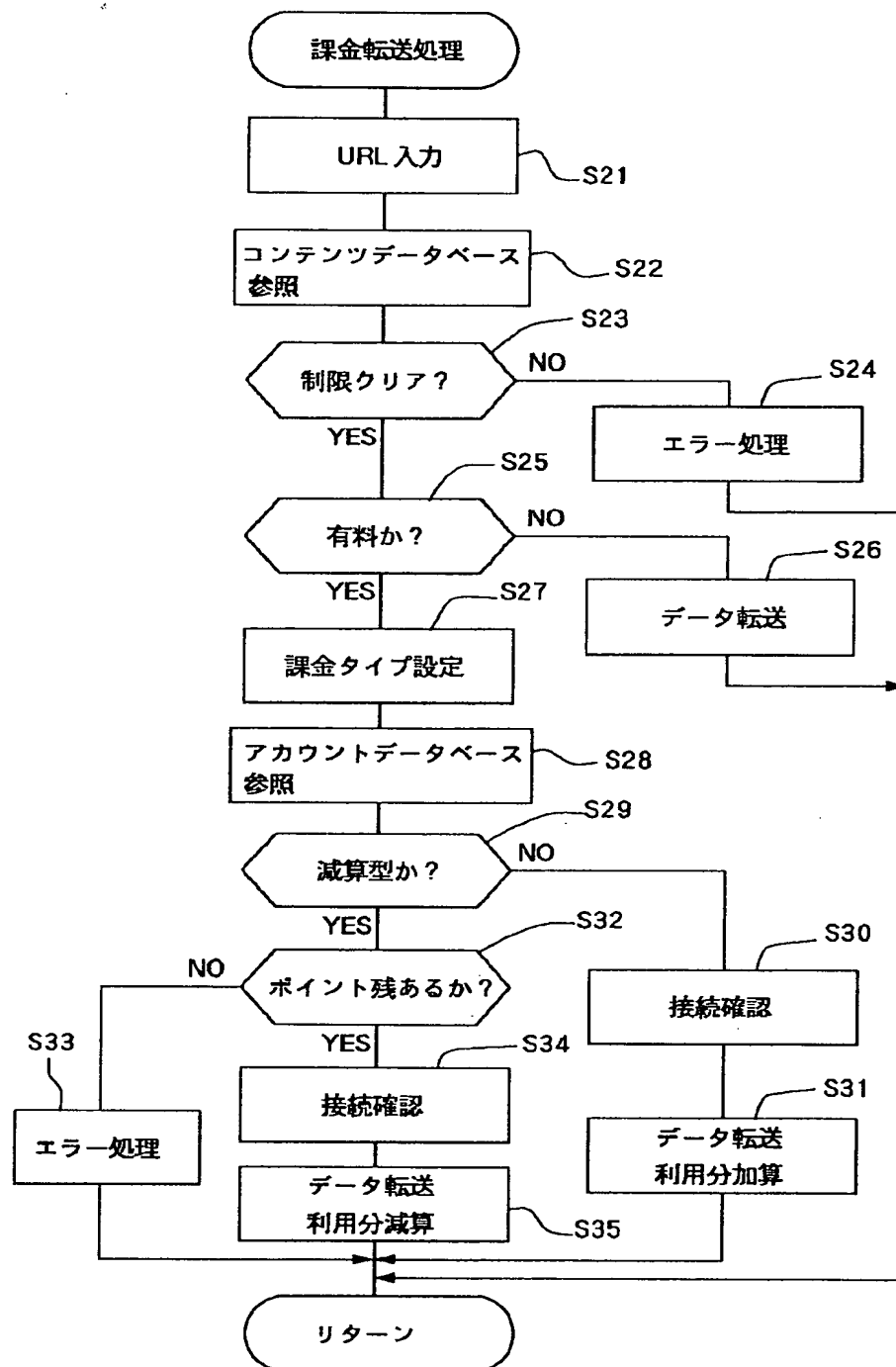
【図5】



【図7】



【図8】



【図9】

